KRIEG DEVAULT

Insights

Health Care Provider agrees to $2.14 million HIPAA Settlement

November 20, 2016

By: Stacy Walton Long

St. Joseph Health ("St. Joseph"), a nonprofit Catholic health care delivery system, purchased a new server to store files, including electronic Protected Health Information ("ePHI"), that incorporated a file sharing application. The default settings of the new server allowed anyone with an internet connection to access these files via internet search engines. St. Joseph implemented this new server without thoroughly examining the potential risks to ePHI. As a result, certain files that St. Joseph created, which included ePHI, were publicly accessible on the internet, without restriction, from February 1, 2011 to February 13, 2012.

On February 14, 2012, St. Joseph reported this inadvertent disclosure of ePHI to the U.S. Department of Health and Human Services, Office for Civil Rights ("OCR"). OCR investigated the incident and discovered potential violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Security Rules. Specifically, OCR found:

- St. Joseph potentially disclosed the ePHI of 31,800 patients from February 1, 2011 to February 13, 2012
- The security of the ePHI was potentially compromised due to St. Joseph's failure to conduct a thorough evaluation of the implementation of the new server
- St. Joseph failed to perform an "enterprise-wide risk analysis," as required by HIPAA and the Security Rules

In light of these potential violations, St. Joseph agreed to settle the potential violations for $2,140,500 and to adopt a comprehensive corrective action plan. The corrective action plan will require St. Joseph to "conduct an enterprise-wide risk analysis, develop and implement a risk management plan, revise its policies and procedures, and train its staff on the policies and procedures."

This incident and the expensive consequence is an important lesson for healthcare providers. It is vital that a comprehensive risk analysis is performed, but also that providers evaluate and address potential security risks when implementing any changes to their internal systems. Further, it is crucial to have policies and procedure in place regarding the storage of ePHI, and training on such policies and procedures.

When dealing with ePHI, the Information Technology (IT) department of the healthcare provider should be involved in implementing any changes to the internal storage system of ePHI and evaluating the security of such system. Further, the IT department should be aware and trained on the policies and procedures regarding storage of ePHI so they can determine any potential security risks to ePHI that others might not be able to foresee.

If you have any questions, please contact Stacy Walton Long.